BOISE MATTHEWS LLP
Bridget M. Donegan, OSB No. 103753
805 SW Broadway, Suite 1900
Portland, OR 97205
(503) 228-0487
bridget@boisematthews.com

Attorneys for Plaintiff Loujain Hathloul Alhathloul

FOLEY HOAG LLP
Christopher E. Hart, MA BBO No. 625031
chart@foleyhoag.com
Anthony D. Mirenda, MA BBO No. 550587
adm@foleyhoag.com
Andrew Loewenstein, MA BBO No. 648074 (*pro hac vice pending)*
aloewenstein@foleyhoag.com
155 Seaport Boulevard
Boston, MA 02210
(617) 832-1232

Attorneys for Plaintiff Loujain Hathloul Alhathloul

ELECTRONIC FRONTIER FOUNDATION
Sophia Cope, CA Bar No. 233428 (*pro hac vice pending)*
sophia@eff.org
David Greene, CA Bar No. 160107
davidg@eff.org
Mukund Rathi, CA Bar No. 330622
mukund@eff.org
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Attorneys for Plaintiff Loujain Hathloul Alhathloul

Table of Contents

Table of Authorities

Cases

Foreign Cases

Statutes

Rules

Other Authorities

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

LOUJAIN HATHLOUL ALHATHLOUL,

Plaintiff,

v.

DARKMATTER GROUP, MARC BAIER, RYAN ADAMS, and DANIEL GERICKE

Defendants.

Civil No. 3:21-cv-01787-IM

PLAINTIFF'S OPPOSITION TO MOTION TO DISMISS AND MEMORANDUM OF LAW IN SUPPORT

REQUEST FOR ORAL ARGUMENT

Plaintiff Loujain Hathloul Alhathloul submits this opposition to Defendants' Motion to Dismiss. For the reasons set forth below, the Court should deny the motion in its entirety.

INTRODUCTION

Loujain Alhathloul is a preeminent Saudi human rights activist and leader in the movement to promote the rights of women and girls in the Saudi Arabia. This action arises out of the unlawful actions by Defendant DarkMatter Group ("DarkMatter") and its former senior executives—Marc Baier, Ryan Adams, and Daniel Gericke ("Individual Defendants")—to hack Alhathloul's iPhone, surveil her movements, and exfiltrate her confidential communications for use against her by the security services of the United Arab Emirates ("UAE"). Defendants carried out these actions using cyber-technology developed in the United States, purchased from U.S. companies, and designed to target Apple's servers in the United States. Defendants' tortious actions against Alhathloul caused her arbitrary arrest and rendition to Saudi Arabia, where she was detained, imprisoned, and tortured. Alhathloul brings this action to hold Defendants liable

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

for their violations of the Computer Fraud and Abuse Act ("CFAA") and Alien Tort Statute ("ATS").

Defendants move to dismiss the Complaint for lack of personal jurisdiction, failure to state a claim under the CFAA, lack of subject matter jurisdiction under the ATS, and on the basis that Defendants are entitled to common law conduct-based immunity. None of these grounds have merit.

First, Defendants' abundant U.S.-based and U.S.-targeted activities created sufficient minimum contacts with the U.S. for the Court to exercise jurisdiction over Defendants. Defendants used sophisticated U.S. cyber-technology to target U.S. servers in their hack against Alhathloul, rendering their argument that Alhathloul's allegations amount to an "attempt to manufacture jurisdiction" based merely on "sending a text message" unavailing. Second, Alhathloul's Complaint states a plausible CFAA claim anchored in established facts and reasonable inferences. Indeed, the majority of Alhathloul's allegations draw on facts already admitted as true by the Individual Defendants in a 24-page Factual Statement ("DPA Facts") filed in U.S. court as part of their Deferred Prosecution Agreement ("DPA") with the U.S. Department of Justice.[1] Third, and for many of the same reasons this Court has personal jurisdiction, the Court has subject matter jurisdiction over the ATS claim, which touches and concerns the territory of the United States. Finally, Defendants are not entitled to foreign-official immunity under common law.

[1] Attached as Exhibit A is the DPA and corresponding Factual Statement, which were filed in the U.S. District Court for the District of Columbia, Case No. 1:21-cr-00577, Dkt. 4. Plaintiff requests that the Court take judicial notice of this as a federal court filing. Fed. R. of Evid. 201(b) (court "may judicially notice of a fact that is not subject to reasonable dispute because it. . .can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned"); Fed. R. of Evid. 201(c)(2); *Reyn's Pasta Bella, LLC v. Visa USA, Inc.,* 442 F.3d 741, 746 fn. 6 (9th Cir. 2006) ("We may take judicial notice of court filings. . .").

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Defendants' Motion to Dismiss should be denied in its entirety.

BACKGROUND

A. Defendants' U.S.-based and Targeted Activities are Key Elements of Each of Alhathloul's Claims.

Defendants' contacts with the United States are abundant, material, and indisputable.[2] These contacts support both this Court's exercise of personal jurisdiction over Defendants and the touch and concern element of Alhathloul's ATS claim:

- To carry out their illegal cyber-surveillance, the Individual Defendants, who are *U.S. Persons*, transferred *U.S. technology and knowhow developed by a U.S. company* while the Individual Defendants were *U.S.-based employees* of that company to DarkMatter, a UAE company, and UAE persons, all in violation of U.S. law. Export of this technology to a UAE company or to UAE persons required U.S. Export licenses that the Individual Defendants did not seek or obtain. DPA Facts ¶¶ 32–33.

- Defendants purchased *from other U.S. companies* specialized hacking technology—"zero click" exploits—and fashioned these exploits together with the other U.S. technology described above into a sophisticated hacking system known as "Karma." DPA Facts ¶¶ 44, 66.

- Defendants recruited *U.S. individuals* with cyber-expertise to assist with creating Karma. DPA Facts ¶ 35.

- Defendants' Karma system targeted vulnerabilities in Apple's iMessage system, which operates exclusively on *Apple's iMessage servers located in the United States*, to deliver malware to, and install malware on, Alhathloul's iPhone without her taking any action. DPA Facts ¶ 45; Complaint ("Compl.") ¶ 104.

- Defendants procured and utilized *other U.S. services and technology* to make Karma more effective, including anonymization services *located in the U.S.* to evade detection and attribution of their attacks. DPA Facts ¶ 56.

- Defendants created inauthentic Apple iMessage accounts that they used to obtain Alhathloul's personal account information using *U.S. servers*. DPA Facts ¶¶ 39, 42; Compl. ¶ 104.

- Defendants targeted *Apple's U.S. servers* with exploitive code to commit their hack, including causing Apple's iMessage servers to send an exploit and malware to Alhathloul's iPhone. DPA Facts ¶ 56; Compl. ¶ 104.

[2] The DPA prohibits the Individual Defendants from disputing these facts. *See* DPA ¶ 38.

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

- The Individual Defendants entered into a DPA, in which they admitted to managing, supervising, directing and leading offensive cyber-operations to "gain unauthorized access to, and to thereby acquire data from, computers, electronic devices, and servers…including on computers and servers in the United States, as well as computers and servers that communicated with computers in the United States." DPA Facts ¶¶ 1, 58–60.

B. Defendants Developed and Operated Project Raven to Enable UAE Officials to Target Perceived Dissidents, Including Human Rights Activists.

As part of the UAE's goal to develop advanced cyber-intelligence capabilities, it hired U.S. corporations and recruiting U.S. individuals with expertise in cyber-surveillance. Compl. ¶ 50. In or about 2009, the UAE sought out Maryland-based contractor CyberPoint International LLC ("CyberPoint") to advise on and assemble a program for enhancing the UAE's cyber-capabilities. Compl. ¶ 52. The Individual Defendants, while working for CyberPoint, developed and operated what would come to be known as "Project Raven"—a cyber-surveillance program that targeted perceived dissidents designated by UAE officials, including at the behest of the UAE's regional ally Saudi Arabia. Compl. ¶¶ 46, 60–61.

As CyberPoint employees, the Individual Defendants' activities were governed by U.S. law, including in particular the terms of U.S. export licenses issued by the U.S. Department of State pursuant to the International Traffic in Arms Regulations ("ITAR"). DPA Facts ¶ 32. The export licenses permitted CyberPoint to provide certain defensive cybersecurity services to the UAE, but prohibited U.S. individuals from sharing the technology with UAE companies or persons, and from engaging in offensive cyberattacks or targeting U.S-based servers. DPA Facts ¶ 32. Despite these restrictions, the Individual Defendants developed and operated Project Raven to target and hack individuals and organizations designated by the UAE, including human rights activists, journalists, academics, and other perceived dissidents. Compl. ¶ 60.

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

C. Defendants Relied on U.S. Technology and Knowhow to Develop and Operate Project Raven and Transferred This Technology and Knowhow in Violation of U.S. Law.

Beginning in or about December 2015 through February 2016, the UAE transitioned cyber-services under Project Raven from CyberPoint to UAE-based DarkMatter. Compl. ¶ 67. This involved transferring key Project Raven personnel, including the Individual Defendants, as well as the transfer of U.S. technology and knowhow, all in violation of U.S law. DPA Facts ¶¶ 32–36.

Effective on or about December 31, 2015, the Individual Defendants ceased working for CyberPoint and became employees of DarkMatter. Compl. ¶ 67. As described in the DPA, during this transition process, the Individual Defendants illegally transferred U.S. technology and knowhow—without the necessary U.S. export licenses and in violation of U.S. law—to DarkMatter in the UAE. DPA Facts ¶¶ 32–33. The Individual Defendants recruited other CyberPoint U.S. employees to join DarkMatter. DPA Facts ¶ 35. Following their transition, the Individual Defendants did not seek or obtain licenses from the Department of State allowing them to continue providing services to the UAE or UAE companies or personnel, much less the offensive hacking targeting U.S computers such as the Apple servers that had always been prohibited under even the U.S. export licenses granted to Cyberpoint. Regardless, the Individual Defendants continued to adopt the hacking protocols developed under CyberPoint for DarkMatter. Compl. ¶¶ 69, 73; DPA Facts ¶ 30.

At DarkMatter, the Individual Defendants continued to access and use U.S. technology and knowhow to conduct hacking operations. DPA Facts ¶ 36.

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

D. Defendants Acquired Specific Exploits from the United States Designed to Hack iPhone Users by Targeting U.S. Servers.

As Project Raven became more advanced, Defendants sought new ways to surveil perceived dissidents, including by obtaining remote access to their smartphones. DPA Facts ¶ 44. This led Defendants to purchase two "zero-click" iMessage exploits from companies in the U.S. and to weaponize these exploits against Apple's U.S. servers and iPhone users. DPA Facts ¶ 45. DarkMatter paid approximately $750,000 and $1,300,000, respectively, for each exploit by transferring funds from bank accounts outside the U.S. to bank accounts belonging to the U.S. companies in the United States. Compl. ¶ 84.

Defendants combined these exploits with other features—malware that could control a target's iPhone, and anonymization services located in the United States to evade detection and attribution—to create a hacking system known as "Karma." DPA Facts ¶ 56. Defendants used Karma to "gain unauthorized access to, and to thereby acquire data from, computers, electronic devices, and servers…including on computers and servers in the United States, as well as computers and servers that communicated with computers in the United States." DPA Facts ¶ 1.

1. Defendants Acquired Zero-Click Exploits.

A "zero-click" exploit—such as the one used by Karma—is a specialized type of computer code that leverages flaws in a computer's operating system to execute an action or command (like the installation of malware) without the device owner taking any action, such as clicking a link or navigating to a website. DPA Facts ¶ 56. Defendants chose to use exploits that took advantage of vulnerabilities in Apple's Messages application that runs iMessage. DPA

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Facts ¶ 44. Apple's iMessage system operates through servers located in the United States. DPA Facts ¶ 44.

Defendants' "zero-click" iMessage exploit capitalized on two features of the iMessage system that made it particularly effective for targeting iPhone users. The first feature—the fact that the Messages application is automatically installed on every device running Apple's operating system—allowed Defendants to use the exploit against *any* iPhone user. DPA Facts ¶ 45. The second feature—the fact that iMessage, by design, automatically processes all incoming messages and attachments through Apple's U.S. servers, Compl. ¶ 98—made Defendants' transmission mechanism highly effective. Indeed, Defendants' Karma system successfully compromised a target's device in 90 to 95 percent of deployments, *see* DPA Facts ¶ 57, and without the target taking any action. Compl. ¶ 98; DPA Facts ¶ 51.

Once Defendants deployed their exploit through Apple's U.S. servers and reached a target's device, the exploit leveraged at least two "bugs" in the Messages application. First, the exploit leveraged a vulnerability to "interrupt" the application before it displayed a notification to the iPhone user (*e.g.*, "New message from ..."), which would alert the target that their phone received a suspicious message. Compl. ¶ 98. This allowed Defendants to hack a target without their knowledge. Second, the exploit could run additional stages of exploitive code to circumvent the device's privilege restrictions to ultimately gain access to all data on the iPhone. Compl. ¶ 99-100.

2. Defendants Used Zero-Click Exploits to Attack Apple's U.S. Servers and Compromise Their Targets' iPhone.

Because their chosen exploit was designed to and did rely on vulnerabilities in Apple's iMessage system, Defendants intentionally interacted with Apple U.S. servers several times to successfully deploy a hack. Compl. ¶ 96.

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

First, Defendants had to register for an Apple iMessage account and input the email address or phone number linked to the target's Apple account into Karma. Compl. ¶ 97. Second, in order to send the exploit-containing iMessage, Defendants had to retrieve the target's encryption and routing information from Apple's identity servers—a group of servers located in the U.S. and on which Apple stores encryption and routing information for iMessage users. Compl. ¶ 97. Third, Defendants had to send the exploit-containing iMessage to Apple's iMessage servers to reach their target's iPhone with the exploit and malware. Compl. ¶ 98.

Thus, using Karma, Defendants obtained, without authorization, a targeted individual's log-in credentials and authentication tokens (*i.e.*, unique digital codes issued to authorized issuers) issued by U.S. companies, including computing services, and used these credentials and tokens to exfiltrate data back to DarkMatter without the target's knowledge. DPA Facts ¶ 38. Defendants carried out these activities using, among other things, anonymization services located in the U.S., computer hardware that was bought in the U.S., and email, social media, and server infrastructure accounts from U.S. companies. DPA Facts ¶¶ 38–39.

E. Alhathloul's Advocacy Made Her a Target for Defendants' Hack.

Alhathloul has been an advocate on behalf of women and girls in Saudi Arabia since 2013. Compl. ¶ 16. She has led campaigns supporting the Saudi women's rights movement and rose to prominence by launching a campaign to give women the right to drive. Compl. ¶ 16. Because Alhathloul carried out her activism in her own name, rather than through a pseudonym, she quickly became the public face of the Saudi women's movement. Compl. ¶ 18.

For years, the Saudi government closely monitored and openly condemned Alhathloul's activities. Compl. ¶¶ 19–23.

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

In March 2018, the UAE government targeted Alhathloul and hacked into her iPhone as part of its long-standing cooperation with the Saudi government to persecute perceived dissidents through, among other things, sharing information, security-related cooperation, and the rendition of perceived dissidents. Compl. ¶¶ 45–46, 47–49, 106–07, 114. Both the UAE and Saudi Arabia engage in widespread persecution of perceived dissidents. Compl. ¶¶ 28, 31–41, 50. Together the governments also jointly target individuals who peacefully express views that question or challenge their respective autocratic regimes, including women's rights activists. Compl. ¶ 38, 42–44, 49–51. Following the hack of Alhathloul's iPhone, she was arrested arbitrarily in the UAE and rendered to Saudi Arabia, where she was detained and tortured. Compl. ¶ 26, 27–30, 38, 114, 116–21.

F. Through Project Raven, Defendants Used Karma to Hack Alhathloul and Exfiltrate Her Confidential Communications.

Project Raven used Karma to hack into the iPhones of hundreds of perceived dissidents, including Alhathloul's. Compl. ¶¶ 106–07. During the course of their surveillance, Defendants assigned her the codename "Purple Sword." Compl. ¶ 107.

As alleged and well-pleaded in the Complaint, using Karma, Defendants targeted Apple's iMessage system and weaponized Apple's U.S. servers to carry out their hack against Alhathloul. Compl. ¶ 78, 107–09. Defendants opened fake accounts with Apple to seize Alhathloul's iMessage credentials from Apple's U.S. servers, and then attacked Apple's U.S. servers with its exploit and malware. Compl. ¶¶ 103–05. To compromise the security features on Alhathloul's iPhone protecting confidential information, Defendants knowingly and intentionally sent its malicious code into the U.S. and onto U.S. servers. *Id.*

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

G. Defendants' Hack Against Alhathloul Supported Her Arrest by UAE Security Services and Rendition to Saudi Arabia Where She Was Detained and Tortured.

Defendants' hack against Alhathloul immediately preceded her arrest and rendition to Saudi Arabia. Compl. ¶ 107. The UAE and Saudi Arabia's cooperation in persecuting perceived dissidents was well known at the time of Defendants' hack. Compl. ¶¶ 42–43, 62–64, 114. The UAE and Saudi Arabia cooperated in the persecution of their respective perceived dissidents under intelligence-sharing agreements. Compl. ¶¶ 45–46. In turn, Project Raven met regularly with UAE's National Electronic Security Authority to receive designated targets. Compl. ¶ 62.

Defendants' hack allowed UAE security services to track Alhathloul's whereabouts and monitor her activities. Compl. ¶¶ 1–2. As a result, UAE security services arrested and arbitrarily detained Alhathloul on March 13, 2018, and rendered her to Saudi Arabia. Compl. ¶ 26. She subsequently suffered a series of abuses at the hands of the Saudi government. Compl. ¶ 27. Various Saudi authorities placed her on a travel ban, raided her family home in Riyadh, and arrested and transferred to her to multiple prison facilities. Compl. ¶ 27. At a secret prison in Jeddah, Saudi authorities interrogated Alhathloul and tortured her, including subjecting her to electric shocks and beatings. Compl. ¶ 27. During her interrogation and torture, her interrogators mentioned details regarding her communications that were available through unlawful access of her electronic device. Compl. ¶125. Following her arrest, Saudi Arabia held Alhathloul without charges or trial for ten months. Compl. ¶ 29. Alhathloul was ultimately tried by the Specialized Court of Saudi Arabia; her charging documents referenced private communications stored on her iPhone, including private communications between Alhathloul and other human rights activists that had been transmitted via Telegram and WhatsApp, both end-to-end encrypted messaging services. Compl. ¶ 128–129.

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Defendants' hack against Alhathloul impaired the integrity of the data and security on her iPhone. As a result, she suffered damage to her device and loss aggregating at least $5,000 in value (including the costs incurred due to responding to the hack, conducting a damage assessment, and attempting to restore data). Compl. ¶¶ 153–154. In addition to that loss caused by harm to her iPhone, Alhathloul suffered other loss as a consequence of the hack: Alhathloul lost access to files located on her device, her business contract worth over $2,722 USD per month was cancelled, her vehicle was impounded, and her life, schooling, and career of activism was disrupted. Compl. ¶¶ 156–159.

STANDARD OF REVIEW

To defeat a Rule 12(b)(2) dismissal for lack of personal jurisdiction, the plaintiff need only identify "facts that if true would support jurisdiction." *Ballard v. Savage*, 65 F.3d 1495, 1498 (9th Cir. 1995).

In considering a motion to dismiss under Rule 12(b)(6), the Court must "accept [Plaintiff's] allegations as true and construe them in the light most favorable to plaintiff[]." *Curry v. Yelp Inc.*, 875 F.3d 1219, 1224 (9th Cir. 2017). The same standard applies for Defendants' motion to dismiss arguments under Rule 12(b)(1), as Defendants present a facial, not factual attack, and "argue that the allegations in [the] complaint are insufficient on their face to establish subject matter jurisdiction." *Wolfe v. Strankman*, 392 F.3d 358, 362 (9th Cir. 2004).

ARGUMENT

I. DEFENDANTS HAVE SUFFICIENT MINIMUM CONTACTS WITH THE UNITED STATES.

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Because Alhathloul asserts claims under federal law, and Defendants have maintained they are not subject to general jurisdiction anywhere in the United States,[3] the relevant jurisdictional question is whether Defendants have sufficient "minimum contacts" with the U.S. as a whole such that "the maintenance of the suit does not offend traditional notions of fair play and substantial justice." *Freestream Aircraft (Berm.) Ltd. v. Aero Law Grp.*, 905 F.3d 597, 602 (9th Cir. 2018); *see* Fed. R. Civ. P. 4(k)(2).

The minimum contacts test requires that a defendant either perform some act by which the defendant became purposefully availed of the forum, or alternatively, purposefully direct activities at the forum. *Freestream*, 905 F.3d at 603. The plaintiff's claim must also "arise out of or relate[] to" this conduct, and the exercise of jurisdiction must be reasonable. *Id.*

Purposeful availment and purposeful direction are "distinct" inquiries for assessing minimum contacts. *Pebble Beach Co. v. Caddy*, 453 F.3d 1151, 1155 (9th Cir. 2006). The "key" distinction between these two inquiries is "where the allegedly wrongful conduct took place." *Climax Portble Mach. Tools, Inc. v. Trawema GmbH*, No. 3:18-cv-1825-AC, 2020 U.S. Dist. LEXIS 47790, at *5 (D. Or. Mar. 19, 2020). Purposeful availment is satisfied when a defendant commits tortious conduct inside the forum; purposeful direction applies when a defendant commits tortious conduct outside the forum with intended effects inside the forum. *Id.*

[3] Defendant Adams states in his Declaration that he is not a resident of Oregon, but does not provide an alternative forum state where he would be subject to general jurisdiction. Accordingly, and similar to the other Individual Defendants, Ryan Adams would be subject to jurisdiction under Rule 4(k)(2) if his contacts satisfy the minimum contacts test with the U.S. as a whole. *United States v. Aquatherm GmbH*, No. 3:21-cv-335-JR, 2022 U.S. Dist. LEXIS 117599, at *12 (D. Or. July 5, 2022) (because defendant failed to assert "it was subject to personal jurisdiction in any other state[]" the court could assess personal jurisdiction under Rule 4(k)(2)).

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Defendants' conduct satisfies both purposeful availment and purposeful direction. Defendants purposefully availed themselves of U.S. jurisdiction by committing tortious activity inside the United States through their knowing and deliberate attack against Apple's U.S. servers. Acting through the internet, Defendants obtained Alhathloul's iMessage credentials from Apple's U.S. servers, attacked Apple's U.S. servers with malicious code, and routed these communications through anonymization services located in the United States. Defendants also purposefully directed these actions at servers in the United States and caused harm in the forum by causing Apple's U.S. servers to transmit malicious code to Alhathloul. Defendants' professional backgrounds and expertise, and their involvement in and understanding of the creation of Karma, support the inference that their use of Apple's U.S. servers was a deliberate, purposeful targeting—not the incidental use of servers by the average iPhone user.

A. Defendants Purposefully Availed Themselves of U.S. Jurisdiction by Committing their Tortious Hacking Activity in the United States.

Because "physical presence in the forum is not a prerequisite to jurisdiction," courts recognize that even non-physical contacts with the forum show purposeful availment when those contacts comprise part of the tortious act. *Walden v. Fiore*, 571 U.S. 277, 285 (2014); *Paccar Int'l v. Commercial Bank of Kuwait, S.A.K.*, 757 F.2d 1058, 1064 (9th Cir. 1985) (sending "allegedly fraudulent demand for payment" into forum using messenger system satisfied purposeful availment). Jurisdiction is thus proper even if only "part of the alleged tortious conduct" and not the whole of the tort occurred in the forum. *Climax*, 2020 U.S. Dist. LEXIS 47790, at *9–10; *see also HB Prods., Inc. v. Faizan,* No. 19-00487 JMS-KJM, 2022 U.S. Dist. LEXIS 86761, at *41–42 (D. Haw. May 13, 2022) (finding jurisdiction is "not undercut by the fact that Defendant[s] committed some [tortious] actions outside the United States.").

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

By using Karma to target Apple's iMessage servers and "knowingly cause[] the transmission" of malicious code via those U.S. servers to Alhathloul's iPhone, Defendants committed part of their tortious acts in the United States. *See* 18 U.S.C. § 1030(a)(5).

This court's decision in *Climax* exemplifies how a defendant's tortious actions taken through the internet against an in-forum server satisfies purposeful availment. 2020 U.S. Dist. LEXIS 47790, at *16. The court found jurisdiction under purposeful availment when the defendants, while physically located in Germany, "knowingly accessed" servers in the forum to obtain confidential information, then tortiously misappropriated that information outside the forum. *Id.* at *12, 16. Reasoning that "part of the alleged tort of misappropriation" had taken place in the forum—because this was where defendants accessed the server "for an unauthorized and improper purpose"—the court held that defendants purposefully availed themselves of jurisdiction. *Id.* at *16 (citing with approval *Rhapsody Solutions, LLC v. Cryogenic Vessel Alternatives, Inc.*, 2013 U.S. Dist. LEXIS 30758, at *5 (S.D. Texas Mar. 5, 2013) ("Numerous courts have exercised personal jurisdiction over nonresident defendants where the minimum contacts with the forum consisted of committing a tort through accessing a server located in the forum state.")); *see also Wien Air Alaska, Inc. v. Brandt*, 195 F.3d 208, 213 (5th Cir. 1999).

Climax follows numerous other courts that have found a defendant is purposefully availed of the forum by using an in-forum server to commit a tort. *See UMG Recordings, Inc. v. Kurbanov*, 963 F.3d 344, 349, 354 (4th Cir. 2020) (foreign defendant "relied on U.S.-based servers," owned by third-party to host music piracy website); *MacDermid, Inc. v. Deiter*, 702 F.3d 725, 730 (2d Cir. 2012); *Facebook, Inc. v. ConnectU LLC*, No. C 07-01389 RS, 2007 U.S. Dist. LEXIS 61962, at *6, 20 (N.D. Cal. Aug. 13, 2007); *CoStar Realty Info., Inc. v. Meissner*, 604 F. Supp. 2d 757, 766 (D. Md. 2009).

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Defendants used servers in the U.S. at multiple points in their hack against Alhathloul, and therefore availed themselves of the forum. Acting through the internet, Defendants accessed Apple's U.S. servers to acquire Alhathloul's iMessage credentials "for an unauthorized and improper purpose," which were necessary to their tortious hack. *Climax*, 2020 U.S. Dist. LEXIS 47790, at *16. Defendants then attacked Apple's U.S. iMessage servers with its exploit and malware and "manipulate[d]" these servers to "knowingly cause[] the transmission" of malware to Alhathloul's iPhone, in violation of the CFAA. *See* 18 U.S.C. § 1030(a)(5)(A); *HB Prods, Inc.*, 2022 U.S. Dist. LEXIS 86761, at *28. Defendants chose U.S.-developed exploits, individuals recruited from the United States, and anonymization services located in the United States, to create a highly effective hacking system that operated through those U.S. servers.

B. Defendants Purposefully Directed Their Tortious Actions at the United States.

Alternatively, Defendants' conduct satisfies the minimum contacts test for the independent reason that Defendants purposefully directed their tortious actions at the United States. To assess purposeful direction, courts apply a three-part effects test. *Calder v. Jones*, 465 U.S. 783, 790-91 (1984) (requiring an intentional act, that is expressly aimed at the forum, and causes harm that the defendant knows is likely to be suffered in the forum).

These actions, if they are viewed only as occurring outside the United States, would satisfy the "express aiming" element for the same reasons they satisfy purposeful availment: Defendants intentionally aimed their exploit and malware at Apple's U.S. servers to leverage vulnerabilities in Apple's iMessage system and reach Alhathloul's iPhone. The Ninth Circuit, this Court, and numerous others have found express aiming where a defendant uses an in-forum server to commit a tort. *See, e.g.*, *DEX Sys., Inc. v. Deutsche Post AG*, 727 F. App'x 276, 278 (9th Cir. 2018) (defendant used forum-located server to commit copyright infringement);

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Climax, 2020 2020 U.S. Dist. LEXIS 47790 at *20–21; *MacDermid*, 702 F.3d at 730; *Felland v. Clifton*, 682 F.3d 665, 676 n.3 (7th Cir. 2012); *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 826 (N.D. Cal. 2014); *ConnectU*, No. C 07-01389 RS, 2007 U.S. Dist. LEXIS 61962, at *19-20; *Vivint, Inc. v. Bailie*, No. 2:15-CV-685-DAK, 2017 U.S. Dist. LEXIS 13082, at *10 (D. Utah Jan. 30, 2017).

For similar reasons, Defendants caused harm that they knew was likely to be suffered in the forum. Under this effects test, the plaintiff need not suffer the "brunt of the harm" in the forum, only a "jurisdictionally sufficient amount of harm." *Yahoo! Inc. v. La Ligue Contre Le Racisme*, 433 F.3d 1199, 1207 (9th Cir. 2006). By uploading malicious code to Apple's U.S. servers for delivery to Alhathloul's iPhone, Defendants broke the digital security that is critical to Alhathloul's human rights work and transformed Apple's secure messaging system into Defendants' personal malware delivery device. Digital technology is the central way for human rights activists living under repressive governments to communicate and coordinate their work.[4] Apple specifically designs its products to protect these confidential communications.[5] Once Defendants sent their malware to these U.S.-based servers, no further intervention from Defendants was required to complete the hack. This harmful transmission occurred in the United States and thus satisfies the requirement that a "jurisdictionally sufficient" amount of harm occur in the forum, even though the "brunt of the harm" did not occur until Alhathloul's device was fully compromised. *Yahoo! Inc.*, 433 F.3d at 1207.

[4] *Human Rights Watch Among Pegasus Spyware Targets,* HUMAN RIGHTS WATCH (Jan. 26, 2022), https://www.hrw.org/news/2022/01/26/human-rights-watch-among-pegasus-spyware-targets.

[5] *Apple Expands Industry-leading Commitment to Protect Users from Highly Targeted Mercenary Spyware*, APPLE (July 6, 2022), https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/.

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

C. Defendants' Argument Improperly Narrows the Court's Jurisdictional Inquiry.

Defendants do not dispute that their malicious hack reached U.S. servers in order to infect Alhathloul's device, but dispute the jurisdictional significance of these contacts—arguing that, because they claim that their actions were not "expressly aimed at" or "intended to cause harm in" the United States, their actions do not show purposeful direction under *Calder*'s "effects test." Mot. to Dismiss at 6.

As a threshold matter, Defendants' argument about their purported lack of intent is unavailing in light of the Complaint's allegations that they intentionally targeted Apple's servers to hack Alhathloul's iPhone. Compl. ¶¶ 87, 105, 109. Defendants may answer the Complaint and protest their innocence, but that factual dispute is for a jury to resolve. These factual and not facial arguments should carry no weight at the motion to dismiss stage.

In any event, Defendants' exclusive reliance on the effects test and purposeful direction is misplaced. Although the effects test can serve as an important assessment of minimum contacts when a defendant's actions occur exclusively outside the forum, the court need not apply the effects test where, as here, a defendant commits a part of their tortious conduct in the forum. *Freestream*, 905 F.3d at 604–05 ("*Calder* extended the reach of personal jurisdiction" to encompass actions "*outside* the forum state that are directed at the forum, such as the distribution in the forum state of goods originating elsewhere."). As this court explained in *Climax*, when an out-of-forum defendant commits "part of the alleged tortious conduct" in the forum, these contacts should be assessed under purposeful availment, "not the effects test under *Calder*." *Climax*, 2020 U.S. Dist. LEXIS 47790, at *9.

Defendants wrongly argue for application of the effects test merely because "[the] plaintiff's claims sound in tort." Mot. to Dismiss at 5 (internal quotations omitted). But as the

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Ninth Circuit clarified, there is no "rigid dividing line" between tort claims and contract claims. *Glob. Commodities Trading Grp., Inc. v. Beneficio de Arroz Choloma, S.A.*, 972 F.3d 1101, 1107 (9th Cir. 2020). Deciding on which minimum contacts test to apply does not depend on the type of claim at issue. *Id.* (rejecting this rigid distinction because a defendant's meaningful contacts are "[a]t bottom, [what] both purposeful availment and purposeful direction ask.").

Jurisdiction is proper under both tests.

D. Defendants' Contacts With U.S. Servers Were Knowing and Intentional, Not Fortuitous.

Defendants developed a sophisticated hacking system that knowingly exploited Apple's U.S. servers to route, store, and deliver malicious code to Alhathloul. Rather than being "merely fortuitous," Defendants' hack only worked because it had to use Apple's U.S. servers, and "reverse-engineered" and "emulated" Apple's legitimate code to "transmit malicious code over [Apple's] servers." These actions "indicate[] a knowledge of how [Apple's] servers worked and where they were located." *See WhatsApp*, 472 F. Supp. 3d at 649.

Courts have rejected server contacts as being "merely fortuitous"—both under purposeful availment and purposeful direction—where, as here, the defendant knowingly targets U.S. servers to carry out a tort. For example, in *Climax*, this court reasoned that contacts with an in-forum server with "knowledge of its location . . . creates enough minimum contacts to support personal jurisdiction, without analyzing the effects test." *Climax* at *14; *see also MacDermid, Inc. v. Deiter*, 702 F.3d 725, 730 (2d Cir. 2012) (holding purposeful availment met when defendant "used [in forum] servers to send an email which itself constituted the alleged tort" and knew the servers were located in the forum).

The Complaint's allegations leave no doubt that Defendants knew U.S. servers would be used to carry out their hack. Their design and operation of Karma required a deep understanding

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

of Apple's iMessage system and how its U.S. servers were involved. The U.S. Department of Justice describes Defendants as having created "hacking and intelligence gathering systems that leveraged servers in the United States belonging to a U.S. technology company"—Apple—"to obtain remote, unauthorized access" to any person with an Apple phone.[6] This description is supported by the Individual Defendants' factual admissions in the DPA. DPA Facts ¶ 44–45, 56, 66. The record belies any notion that Defendants did not know Apple's U.S. servers would be penetrated with their malicious code. *Oregon Int'l Airfreight Co. v. Bassano*, 2022 U.S. Dist. LEXIS 102322 (D. Ore. May 16, 2022) (finding allegation that defendant knew server's location is sufficient at motion to dismiss stage). On a motion to dismiss, this Court must provide Alhathloul the benefit of all favorable inferences reasonably available from the record, which requires a rejection of Defendants' characterization of their U.S. contacts as benign or incidental.

By contrast, the cases on which Defendants rely share little factual common ground with the actions of sophisticated cyber-spies. For example, in *Hungerstation*, the Ninth Circuit held that jurisdiction over a foreign entity was not proper "solely because" the out-of-forum defendant "remotely access[ed] servers located in the United States." *Hungerstation LLC v. Fast Choice LLC*, 857 F. App'x 349, 351 (9th Cir. 2021). But in *Hungerstation* this remote access occurred only due to defendants entering "their then-valid [log-in] credentials" to a computer terminal located abroad, which transferred data from Hungerstation's servers hosted in the United States to the defendants. *Hungerstation LLC v. Fast Choice LLC*, No. 19-cv-05861-HSG, 2020 U.S.

---

[6] *Three Former U.S. Intelligence Community and Military Personnel Agree to Pay More Than $1.68 Million to Resolve Criminal Charges Arising from Their Provision of Hacking-Related Services to a Foreign Government*, DEP'T OF JUSTICE, OFFICE OF PUBLIC AFFAIRS (Sept. 14, 2021), https://www.justice.gov/opa/pr/three-former-us-intelligence-community-and-military-personnel-agree-pay-more-168-million (last accessed July 20, 2022). This Department of Justice press release of the DPA is available on the government's website and is appropriate for judicial notice under Federal Rule of Evidence 201.

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Dist. LEXIS 5442, at *4 (N.D. Cal. Jan. 13, 2020). Unlike Defendants here, who committed sophisticated attacks on U.S. servers with code that they engineered to use against Apple's U.S. servers, the conduct in *Hungerstation* involved ordinary internet activity—entering a username and password—that any computer user could perform while also remaining oblivious to the location of the relevant servers. When an ordinary internet user is oblivious to the location of a server, it makes sense to assume those server contacts fortuitous because "[m]ost Internet users, perhaps, have no idea of the location of the servers" they are contacting. *MacDermid, Inc. v. Deiter*, 703 F.3d 725, 730. But Defendants here are not ordinary internet users and did not unwittingly reach U.S. servers in their normal course of using iMessage.

Nor did Defendants' U.S. contacts involve "solely" *accessing* Apple's servers. *Hungerstation*, 857 F. App'x at 351. Defendants first designed a hacking system, using U.S. technology and U.S. persons, with the purpose of leveraging Apple's U.S. servers, and then accessed Apple's U.S. servers to obtain and abuse Alhathloul's iMessage credentials. Defendants took the further step of sending and loading their malicious code onto those U.S. servers in order to compromise Alhathloul's device.

For similar reasons, the remaining decisions upon which Defendants rely to support their fortuity argument are inapposite. In each case, there is a clear divergence between the facts that made those server contacts fortuitous and Defendants' actions. *See Broidy Capital Mgt., LLC v. Qatar*, 2018 U.S. Dist. LEXIS 230971 (C.D. Cal. Aug. 22, 2018) (server location was "fortuitous" because plaintiff alleged no facts that defendants targeted the servers or even committed an intentional act); *Future World Elecs., LLC v. Results HQ, LLC*, 2018 U.S. Dist. LEXIS 88979, at *9 (E.D. La. May 29, 2018) (defendant's server access was authorized and not tortious); *Rosen v. Terapeak, Inc.*, 2015 U.S. Dist. LEXIS 198786, at *28 (C.D. Cal. Apr. 28,

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

2015) (defendant merely "obtain[ed]" plaintiff's images from in-forum server and parties failed to "brief the relevance of the location of the servers").

The nature of the sophisticated cyber-attacks against Alhathloul—which involved far more than merely "sending a text message from a location abroad to a phone located abroad"—render Defendants' exaggerated concerns about "essentially universal jurisdiction over a truly breathtaking scope of claims" inapposite. Mot. to Dismiss at 8, 11. Indeed, Defendants' argument would allow cyber-spies who design hacking tools that target U.S. servers to abuse those servers with impunity while "simply pleading ignorance as to where these servers were physically located." *Facebook, Inc. v. ConnectU LLC*, No. C 07-01389 RS, 2007 U.S. Dist. LEXIS 61962, at *19-20 (N.D. Cal. Aug. 13, 2007) (rejecting ignorance about server's location to avoid jurisdiction).

E. The Suit Arises From Defendants' Contacts with the United States.

Alhathloul's claims arise out of or relate to Defendants' contacts with the forum because without these contacts, Defendants could not have completed the hack against her.

For a claim to "arise out of" a defendant's contacts with the forum, there must be "an affiliation between the forum and the underlying controversy, principally, [an] activity or an occurrence that takes place in the forum . . . and is therefore subject to [its] regulation." *Ford Motor Co. v. Montana Eighth Jud. Dist. Ct.,* 141 S. Ct. 1017, 1025 (2021). The Ninth Circuit applies a "but-for" test to "determine whether the plaintiff would not have suffered injury 'but for' the defendant's forum-related conduct." *Oregon Int'l Airfreight Co.*, 2022 U.S. Dist. LEXIS 102322, at *14 (quoting *Adidas Am., Inc. v. Cougar Sport*, 169 F. Supp. 3d 1079, 1092 (D. Or. 2016)).

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Without Defendants' abundant U.S.-based contacts, the hack against Alhathloul's iPhone could not have occurred. Defendants' contacts with U.S. servers—including both their acquisition of Alhathloul's iMessage credentials from Apple's U.S. servers and transmission of exploitive code to Apple's U.S. servers—were necessary to infecting Alhathloul's iPhone with malware.

More broadly, however, Defendants other U.S.-based contacts—including the acquisition of exploits, reliance on U.S. technology and knowhow illegally transferred from CyberPoint, employment of U.S. individuals, and U.S. anonymization services—were essential to the operation of Project Raven and thus to the hack against Alhathloul. Because the activities of Project Raven and the hack against Alhathloul share this important nexus, the "history of DarkMatter, its technology, and its employees" are all relevant to showing how Alhathloul's claims arise out of Defendants' U.S.-based contacts. Mot. to Dismiss at 11.

F. Defendants Fail to Show Jurisdiction is Unreasonable.

Once a plaintiff establishes that the first two prongs of the minimum contacts test are met, the burden shifts to the defendant to demonstrate the exercise of jurisdiction would be unreasonable. *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 476-78 (1985). Defendants fail to meet that burden and raise only mere inconveniences and speculative concerns.

To evaluate reasonableness, the Ninth Circuit applies a seven-factor balancing test, weighing: (1) the extent of the defendant's purposeful interjection into the forum state's affairs; (2) the burden on the defendant of defending in the forum; (3) the extent of conflict with the sovereignty of the defendant's [home forum]; (4) the forum state's interest in adjudicating the dispute; (5) the most efficient judicial resolution of the controversy; (6) the importance of the

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

forum to the plaintiff's interest in convenient and effective relief; and (7) the existence of an alternative forum. *Freestream*, 905 F.3d at 607.

First, as discussed above, Defendants purposefully interjected themselves into the forum by exploiting vulnerabilities in Apple's iMessage system, deliberately transmitting malware into the United States, and commissioning their tortious activity inside the forum. For the reasons identified above, Defendants' interjection into the forum was not fortuitous or accidental.

Second, Defendants raise only a minimal burden of defending this suit in the United States. All of the Defendants are currently involved in other legal proceedings in the United States and are represented by U.S. counsel.[7] *In re Zf-Trw Airbag Control Units Prods. Liab. Litig.*, No. LA ML19-02905 JAK (FFMx), 2022 U.S. Dist. LEXIS 32593, *51 (C.D. Cal. Feb. 9, 2022) (mitigating factor is whether defendant "has some familiarity with the legal system in the United States" or "has retained counsel who are based here"). Notably, the Individual Defendants already conceded to U.S. jurisdiction when they entered into the DPA, and the DPA imposes continual obligations on the Individual Defendants for the term of the agreement. DPA, ¶ 9 (requiring annual disclosures).

This minimal burden must be weighed against the corresponding burden on Alhathloul to litigate in an alternative forum: the UAE. *Sinatra v. Nat'l Enquirer, Inc*., 854 F.2d 1191, 1199 (9th Cir. 1988). There is little doubt that Alhathloul would be unable to receive a fair trial in the UAE, and would likely face threats to her personal safety if she even attempted to bring her claims in UAE court.

[7] DarkMatter is currently co-defendant in *Oueiss v. Al Saud, et. al.*, Case No. 22-11408-AA (11th Cir.); *see also* DPA ¶ 3 (establishing three-year Term, ending on September 14, 2024).

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Third, Defendants merely assert, without further explanation, that "[t]here is an obvious conflict with the sovereignty of DarkMatter's home forum because Plaintiff's allegations concern events that occurred largely in the UAE and directly implicate the UAE government." Mot. to Dismiss at 12. Although Alhathloul's claims relate to conduct carried out at the behest of the UAE government, her claims "seek[] only the determination and enforcement" of U.S. laws against the individuals and private corporations involved, not the UAE itself. *Ayla, LLC v. Alya Skin Pty. Ltd.*, 11 F.4th 972, 984 (9th Cir. 2021). Indeed, essential aspects of the hack occurred in the United States. Although courts must consider the "procedural and substantive interests of other nations" in their decision to exercise jurisdiction, this inquiry commonly focuses on the foreign state's "particular interest in adjudicating th[e] suit." *Asahi Metal Indus. Co. v. Superior Court of Cal.*, 107 S. Ct. 1026, 1034 (1987); *Harris Rutsky & Co. Ins. Servs. v. Bell & Clements Ltd*., 328 F.3d 1122, 1133 (9th Cir. 2003) (identifying adjudicatory interest of sovereign). Defendants fail to identify any such interest the UAE may have in adjudicating the violations of U.S. law carried out by these Defendants in service of the UAE's campaign against dissidents. The only interest that Defendants seem to hint at—the UAE's policy of surveilling perceived dissidents—cannot shield Defendants from answering for violations of U.S. law, as demonstrated by the Individual Defendant's criminal prosecution covered by the DPA.

Fourth, the United States' interest in adjudicating this civil case is compelling. The DPA itself presents clear evidence showing that the United States has an interest in regulating the violations of U.S. law and the harm that occurred in this case, and even anticipates the possibility of civil suits arising out of this conduct. DPA ¶ 24 ("This Agreement does not provide any protection for any. . .civil matter.").

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Fifth, because Alhathloul's claims arise under U.S. federal law and "rest on the law of … the United States," the United States provides "the most efficient judicial resolution of the controversy." *Ayla,* 11 F.4th at 984. Although some "relevant parties, documents, and witnesses" likely are located abroad, many others likely are located in the United States—for example, Apple's technology experts and the companies that designed and sold the exploits used by Defendants. In any event, this factor "is no longer weighed heavily given the modern advances in communication and transportation." *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316, 1323 (9th Cir. 1998).

Sixth, and for the same reasons, this forum is most likely to provide "convenient [and] effective relief" because Alhathloul's claims arise under U.S. law. *Id.* at 1324.

Seventh, Defendants argument faulting Alhathloul for failing to show an alternative forum is unavailing. The burden of demonstrating the lack of an alternative forum "becomes an issue only when the forum state is shown to be unreasonable." *Sinatra v. Nat'l Enquirer, Inc.*, 854 F.2d 1191, 1201 (9th Cir. 1988). Defendants fail to make that showing. In any event, the Complaint's allegations show that the UAE is not a viable alternative forum and because Alhathloul's claims arise under U.S. law, no alternative forum exists.

Defendants fail to meet their burden of demonstrating that the Court's exercise of jurisdiction would be unreasonable.

II. THE COMPLAINT VALIDLY ALLEGES VIOLATIONS OF THE CFAA.

A. Alhathloul's Claims are Anchored in Established Facts and Reasonable Inferences.

To prevail on a motion to dismiss for failure to state a claim, the defendant must show "there is no cognizable legal theory to support the claim" or that "the complaint lacks sufficient factual allegations to state a facially plausible claim for relief." *Murphy v. United States*, 2022

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

U.S. Dist. LEXIS 2299, at *2-3 (D. Or. Jan. 5, 2022) (citing *Shroyer v. New Cingular Wireless Servs., Inc.*, 622 F.3d 1035, 1041 (9th Cir. 2010)). The complaint must plead facts that, if accepted as true, would "state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Determining the plausibility of a claim requires the court to consider "the entire factual context" of the complaint. *Park v. Thompson*, 851 F.3d 910, 928 (9th Cir. 2017) (considering "entire factual context" to find the plaintiff "nudged [her] claim . . . across the line from conceivable to plausible") (internal quotations omitted).

While the Court is required, at the motion to dismiss stage, to accept as true Alhathloul's allegations, the vast set of facts that have already been admitted by the Individual Defendants in U.S. court make this case different. These facts conclusively establish that Defendants operated Project Raven to hack individuals identified by the UAE, including human rights activists and other perceived dissidents, and used zero-click exploits in a system known as Karma to hack into the iPhones of hundreds of targets. DPA Facts ¶¶ 42–44. The Individual Defendants held key supervisory positions at DarkMatter and further admitted to adopting the hacking protocols developed under CyberPoint for Project Raven in order to continue to target perceived dissidents of the UAE and Saudi Arabia. DPA Facts ¶¶ 25–27, 60.[8]

Beyond the facts admitted in the DPA, the Complaint cites credible reporting from *Reuters* that connects Alhathloul to the very conduct Defendants admitted to in the DPA: "Project Raven targeted and hacked Alhathloul" and during the course of this surveillance "assigned her the code name 'Purple Sword.'" Compl. ¶ 107. *Reuters*' extensive reporting about Project Raven and these Defendants was "based on interviews with whistleblowers who

[8] Faced with these admissions, Defendants can only argue that the DPA "makes no mention of Plaintiff." Mot. to Dismiss at 15. Of course, the DPA makes no mention of *any* individual victim.

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

previously worked on Project Raven and an independent review of Project Raven documents." Compl. ¶ 106. These allegations drawn from *Reuters* are particularly credible when considered in light of the facts admitted in the DPA, and together provide a reasonable basis for inferring that Defendants committed the alleged violations. *See In re Wet Seal, Inc. Sec. Litig.*, 518 F. Supp. 2d 1148, 1172 (C.D. Cal. 2007) ("[N]ewspaper articles should be credited . . . if they are sufficiently particular and detailed to indicate their reliability.") (quoting *In re McKesson HBOC, Inc. Secs. Litig.*, 126 F. Supp. 2d 1248, 1272 (N.D. Cal. 2000)). Defendants neither contest the veracity of this reporting from *Reuters*, nor make any specific mention of it in their Motion to Dismiss.

Although Alhathloul's allegations are anchored in these established and otherwise credible facts, Defendant's seek to summarily dismiss them as "speculative." Mot. to Dismiss at 15. But, as this court recognized, information and belief allegations are "a desirable and essential expedient when matters that are necessary to complete the statement of a claim are not within the knowledge of the plaintiff but he has sufficient data to justify interposing an allegation on the subject." *Covelli v. Avamere Home Health Care LLC*, No. 3:19-cv-486-JR, 2021 U.S. Dist. LEXIS 57037, at *10 (D. Or. Mar. 25, 2021) (quoting 5 Charles Alan Wright & Arthur R. Miller, Federal Practice and Procedure § 1224 (2d ed. 1990)). Indeed, courts in this Circuit "relax pleading requirements where the relevant facts are known only to the defendants" and a plaintiff need not specifically plead facts to which she cannot be "reasonably expected to have access." *Concha v. London*, 62 F.3d 1493, 1503 (9th Cir. 1995). To the extent the Complaint relies on an "information and belief" allegation to infer the Individual Defendants' culpability, that is necessary because she cannot be "reasonably expected to have access" to information about the inner workings of Project Raven, which by design was meant to be a covert operation.

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

The Complaint's allegations, considered in the "entire factual context," provide a reasonable basis for alleging Defendants' committed these CFAA violations against the Plaintiff. The Complaint provides a detailed account of Defendants' manner, motive, and method of the hacking activity that plausibly connects it to the CFAA violations committed against her. These allegations are not speculative regarding DarkMatter's participation, and contrary to Defendants' argument, do provide a factual basis for concluding that the Individual Defendants participated in the hacking of Alhathloul's iPhone. Mot. to Dismiss at 15.

B. Alhathloul's Claim Meets the Requirements for a CFAA Civil Claim.

The CFAA authorizes a civil cause of action when a person "suffers damage or loss by reason of a violation" of the statute, and that violation causes either (1) financial loss greater than $5,000; or (2) physical harm. *See* 18 U.S.C. § 1030(g); 18 U.S.C. § 1030(c)(4)(A)(i).

Alhathloul plausibly alleges that the hack both caused her physical injury and financial loss greater than $5,000. Compl. ¶¶ 153-163.

Defendants do not dispute that Alhathloul's Complaint alleges she was detained and tortured as a result of the hack. Nor do they dispute that she alleges damage to her iPhone—a protected device under the CFAA—because the hack compromised the integrity of the security features on her iPhone. *See* 18 U.S.C. § 1030(e)(8) (defining damage as "any impairment to the integrity or availability of data, a program, a system, or information").

1. Defendants' Conduct Caused Alhathloul's Physical Injury.

The Complaint's allegations draw a direct line between the digital crimes perpetrated against Alhathloul and the physical injury she suffered. Defendants' hack led UAE security services to arrest Alhathloul, and predictably caused Saudi Arabia to detain and torture her.

a. Alhathloul's Physical Injury was a Direct and Foreseeable Result of Defendants' CFAA Violations.

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

To determine whether Defendants' hack caused Alhathloul's physical injury, this Court must determine whether "some direct relation" exists between the hacking and surveillance of Alhathloul and her arrest, detention, and torture. *Bank of Am. Corp. v. City of Miami*, 197 L. Ed. 2d 678, 690 (2017).

Here, Plaintiff's physical injury was a direct consequence and foreseeable result of the CFAA violation committed against her. Defendants do not dispute that Alhathloul's Complaint alleges the unauthorized access to her device was a cause-in-fact of her physical injury. *See* Mot. to Dismiss at 20-21 ("To be sure, the Complaint alleges that the Saudi forces used information obtained through the alleged hacking to target and locate Plaintiff."). Instead, they argue that the action of Saudi officials was an "independent, intervening cause" that severs liability. *Id.* at 20. But not all intervening actions sever liability. Rather, "to qualify as a superseding cause so as to relieve the defendant from liability for the plaintiff's injuries, both the intervening act and the results of that act must not be foreseeable." *Fraser v. Mint Mobile, LLC*, No. C. 22-00138 WHA, 2022 U.S. Dist. LEXIS 76772, at *9 (N.D. Cal. Apr. 27, 2022); *Ileto v. Glock Inc.*, 349 F.3d 1191, 1209 (9th Cir. 2003) ("[A]n intervening act does not amount to a 'superseding cause'. . . if it was reasonably foreseeable.").

Courts have recognized that acts of a third-party "do not qualify as superseding causes" when they arise from a known or reasonably anticipated threat. *Id.* In *Fraser*, the court found that the defendant's alleged CFAA violation—bypassing the plaintiff's pin verification set up on his mobile account—could be reasonably anticipated to cause third-party cryptocurrency theft because it made swapping SIM cards easier and "SIM hijacking represent[ed] a national problem." *Id.* (assessing "proximate cause" for "all counts" before assessing whether the theft qualified as a predicate loss).

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

In the present case, the actions of both UAE and Saudi officials should clearly have been reasonably anticipated by Defendants, who surveilled dissidents at the behest of foreign nations with a pattern of human rights abuse. The Complaint identifies dissidents DarkMatter surveilled who were later arrested; there are likely others. If anything, Alhathloul's physical injury is more foreseeable than the theft in *Fraser*, where defendants could at least point to intervening acts of a not-yet-identified third-party. Defendants' activity was closely intertwined with the state actors that inflicted her injury: Defendants participated in meetings with government officials who identified hacking targets and specifically targeted government dissidents with histories of previous arrest, detention, and/or torture.

b. Alhathloul's Physical Injury Need Not Stem From A Technological Harm.

Because Defendants' CFAA violations directly and foreseeably resulted in Alhathloul's physical injury, her injury satisfies the predicate for a civil CFAA claim. Defendants wrongly argue that Alhathloul's physical injury is not cognizable under the CFAA because it does not relate to a "technological harm" or "stem from the unauthorized access itself." Mot. to Dismiss at 19.

These limitations find no basis in the CFAA's statutory language, and Defendants' cited authority only addresses the separate predicate of "loss"—not "physical injury." *See, e.g., Van Buren v. United States*, 141 S. Ct. 1648, 1660 (2021) ("The statutory definitions of 'damage' and 'loss' thus focus on technological harms—such as the corruption of files—of the type unauthorized users cause to computer systems and data."); *see also Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1263 n.10 (9th Cir. 2019) (distinguishing a "predicate 'loss'" necessary for a civil claim from what constitutes recoverable "economic damages" under the CFAA).

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

Defendants try to extend the Supreme Court's decision in *Van Buren*, and this Circuit's decisions in *Andrews* and *Fraser* well beyond their actual holdings, but the CFAA's plain language reflects that physical injury is a distinct type of harm from "loss." Physical injury, as its ordinary and everyday meaning is understood, is separate from "loss"—defined as "any reasonable cost" to a hacking victim. *See* 18 U.S.C. § 1030(e)(11) (listing economic costs a victim may incur).

This distinction is also apparent in the statutory structure of the CFAA. Under 18 U.S.C §1030(c)(4)(A)(i), "loss . . . aggregating at least $5,000 in value" and "physical injury" are separate and sufficient predicates for bringing a civil claim. Interpreting physical injury as synonymous with "loss" would convolute this structure; it would either treat the physical injury predicate as surplusage (when a physical injury resulted in *more* than $5,000 of economic harm) or contradict Congress' intent to set a minimum floor for financial loss claims under the CFAA (when a physical injury resulted in *less* than $5,000 of loss). The only reading that gives the physical injury predicate its full effect is to interpret it as distinct from "loss" and thus untethered to the holdings in *Van Buren*, *Andrews*, and *Fraser*.

This reading is consistent with *Wofse v. Horn*, in which the court held a plaintiff's "anxiety, panic attacks, insomnia, and internal bleeding" as recognized physical injuries caused by the stress induced by defendant's cyber-attacks. 523 F. Supp. 3d 122, 140 (D. Mass. 2021) (denying defendant's motion for summary judgment).

As a last attempt to narrow the physical injury predicate, Defendants point to the CFAA's legislative history—but from an outdated version of the CFAA. Mot. to Dismiss at 20. A critical difference exists between the amended and operative CFAA and the one purporting to support Defendants' argument. Whereas the prior version defined "damage" to include

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

"impairment[s]" that "cause[d] physical injury to any person," the current CFAA is broader: it permits a civil claim if the "conduct involves" physical injury to any person. *Compare* 18 U.S.C. § 1030(e)(8) (1996) *with* 18 U.S.C. § 1030(g). The operative CFAA broadens the inquiry to focus on the consequence of the violation, rather than the damage itself. Even ignoring these critical differences, Defendants' attempt to find support from this outdated statute is unavailing. The statute refers to "impairments" that "cause[] physical injury to any person," pointing directly back to the causation inquiry described above.

2. Defendants' Hack Caused Alhathloul's Financial Loss.

As pleaded in the Complaint, Alhathloul suffered loss aggregating at least $5,000 in value. This loss "includes costs incurred due to responding to the hack, conducting a damage assessment, and attempting to restore data." Compl. ¶¶ 154.

These components are within the CFAA's definition of "loss": "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). Defendants' argument to the contrary thus fails. *See Cantu v. Guerra*, No. SA-20-CV-0746-JKP-HJB, 2021 U.S. Dist. LEXIS 119681, at *15 (W.D. Tex. June 28, 2021) (holding plaintiff satisfied *Iqbal-Twombly* standard by pleading a $5,000 loss to pay retainer to computer forensics companies); *Freedom Banc Mortg. Servs. v. O'Harra*, No. 2:11-cv-01073, 2012 U.S. Dist. LEXIS 125734, at *18-19 (S.D. Ohio Sept. 5, 2012) (finding plaintiff pleaded a $5,000 loss because its computers failed and it lost business). The case to which Defendants point, *Brooks v. Agate Res., Inc.*, has no bearing here, because in that case the plaintiff had not, unlike Alhathloul, specifically alleged a loss of "an amount higher than

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

$5,000." No. 6:15-CV-00983-MK, 2019 U.S. Dist. LEXIS 83681, at *68 (D. Or. Mar. 25, 2019) (subsequent history omitted).

In addition to the costs incurred by Alhathloul, she suffered consequential damages due to the hack, including lost access to files located on her device, the cancellation of a business contract, impoundment of her vehicle, and the disruption to her life, schooling, and career of activism. Compl. ¶¶ 156-160. These consequential damages are cognizable "loss" under the CFAA when they result from the "interruption of service" caused by the hack. 18 U.S.C. § 1030(e)(11) (identifying "other consequential damages incurred because of interruption of service.").

Defendants' hack—although it did not render Alhathloul's phone inoperable—interrupted critical security services on her iPhone. Compl. ¶¶ 101, 152–153. Defendants compromised the iPhone's secure messaging system and other security settings inherent to the device, both of which were critical her human rights work. *Id.* Alhathloul's losses relate directly to the technological harms a human rights activist would suffer when a hack destroys the security of their device. Compl. ¶¶ 156-160.

3. Alhathloul's Conspiracy Claim is Sufficient.

The CFAA creates liability for any person who "conspires to commit" CFAA violations. 18 U.S.C. § 1030(b). In addition to Defendants' direct liability for violating the CFAA, Defendants are liable as co-conspirators. Because the CFAA recognizes "a civil action" for "[a]ny person who suffers damage or loss by reason of a violation of [the CFAA]," courts have recognized that "a plaintiff may pursue a claim for conspiracy under the CFAA if that conspiracy caused damage or loss." *Calsoft Labs, Inc. v. Panchumarthi*, No. 19-cv-04398-NC, 2019 U.S. Dist. LEXIS 194939, at *19 (N.D. Cal. Nov. 7, 2019); 18 U.S.C. § 1030(g). A conspiracy under

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

the CFAA requires an "explicit or tacit understanding or agreement" along with "common activities." *NetApp, Inc. v. Nimble Storage*, 41 F. Supp. 3d 816, 835-36 (N.D. Cal. 2014).

As alleged in the Complaint, the Individual Defendants and DarkMatter reached an actual or tacit agreement, both with each other and the UAE government and its representatives, to commit CFAA violations against numerous human rights activists and perceived dissidents of the UAE and Saudi Arabia. This actual or tacit agreement existed prior to the Individual Defendants' employment with DarkMatter, dating back to their work on behalf of CyberPoint, to implement the hacking protocols under Project Raven. DarkMatter and the Individual Defendants then actually or tacitly agreed to transfer of U.S. technology and knowhow from CyberPoint to DarkMatter. The Individual Defendants, DarkMatter and the UAE government carried out numerous common activities in furtherance of this actual or tacit agreement, including their purchase of "zero-click" exploits to hack Apple's iMessage system and their development of these exploits into the sophisticated hacking system Karma.

Defendants' reliance on the intra-corporate conspiracy doctrine is misplaced. Although many of these common activities occurred during their employment at DarkMatter, the conspiracy itself pre-dates their employment at DarkMatter. *McGraw Co. v. Aegis Gen. Ins. Agency, Inc.*, No. 16-cv-00274-LB, 2016 U.S. Dist. LEXIS 91124, at *21-22 (N.D. Cal. July 13, 2016) ("To the extent [plaintiff] alleges a conspiracy that existed before the defendants entered agency or employment relationships with one another, those allegations are not subject to dismissal under the '"agent's immunity rule."'). As alleged in the Complaint, beginning in or about December 2015 through February 2016, the UAE transitioned cyber-services under Project Raven from CyberPoint to DarkMatter. But the Individual Defendants did not cease their employment at CyberPoint until December 31, 2015, and did not become DarkMatter employees

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

until January 2016. Compl. ¶¶ 69–72. Accordingly, the conspiracy between the Individual Defendants and DarkMatter pre-dates their employment and is not barred by the intra-corporate conspiracy doctrine. Because this conspiracy to commit CFAA violations caused damage or loss to Alhathloul, her conspiracy claim is sufficient.

III. THE COURT HAS SUBJECT MATTER JURISDICTION OVER THE ALIEN TORT STATUTE CLAIM.

A. The Individual Defendants' U.S.-based Conduct Gives Rise to Jurisdiction under the ATS.

Defendants' argument that the Court lacks subject matter jurisdiction over the ATS claim because the claim is impermissibly extraterritorial in nature falls short. The claim sufficiently "touch[es] and concern[s] the territory of the United States" so as to "displace the presumption against extraterritorial application." *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 124-25 (2013). The outcome is no different under the Supreme Court's most recent pronouncement on the ATS, as the Complaint alleges that "conduct that is relevant to the statute's focus occurred in the United States." *Nestlé USA, Inc. v. Doe*, 141 S. Ct. 1931, 1934 (2021) (quoting *RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. 325, 337 (2016)).

Specifically, the Complaint alleges that the Individual Defendants engaged in extensive conduct in the United States relevant to their aiding and abetting, and conspiracy to commit, the crime of persecution. This includes, *inter alia*, the Individual Defendants:

(i) developing a cyber-surveillance program to target perceived dissidents, including human rights activists, while employed by a Maryland-based contractor;

(ii) operating under export licenses acquired from the U.S. Department of State pursuant to the International Traffic in Arms Regulations;

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

(iii) transferring technology and knowhow protected by such U.S. export licenses in violation of federal law;

(iv) recruiting employees from the United States to work on the cyber-surveillance program for DarkMatter;

(v) purchasing "zero click" hacking technology from the United States;

(vi) deploying hacking exploits that targeted Apple's iMessage servers located in the United States;

(vii) incorporating other U.S. technology into the Karma system, such as anonymization services located in the United States;

(viii) obtaining, without authorization, targeted individuals' log-in credentials and authentication tokens issued by U.S. companies;

(ix) opening fake accounts with Apple to seize Ms. Alhathloul's iMessage credentials from Apple's U.S. servers; and

(x) attacking Apple's U.S. servers with exploits and malware by sending malicious code into the United States and onto U.S. servers.

Defendants are not helped by arguing that Alhathloul was "arrested in the UAE and harmed in the UAE and Saudi Arabia." Mot. to Dismiss at 30. The Court must "consider[] a broader range of facts than the location where the plaintiffs actually sustained their injuries." *Al Shimari v. CACI Premier Tech., Inc.*, 758 F.3d 516, 529 (4th Cir. 2014). This is because the Supreme Court in *Kiobel* "broadly stated that the '*claims*,' rather than the alleged tortious conduct, must touch and concern the United States territory with sufficient force, suggesting that courts must consider all the facts that give rise to the ATS claims." *Id*. at 527 (quoting *Kiobel*, 133 S. Ct. at 1669) (emphasis added). *See also id*. at 528 ("("[I]t is not sufficient merely to say

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

that because the actual injuries were inflicted abroad, the *claims* do not touch and concern United States territory.") (emphasis in original); *Jane W. v. Thomas*, 560 F. Supp. 3d 855, 877 (E.D. Pa. 2021) (finding *Kiobel*'s "touch and concern" test satisfied even though the alleged United States-related conduct did not concern the alleged tortious conduct itself); *Sexual Minorities Uganda v. Lively*, 960 F. Supp. 2d 304, 321 (D. Mass. 2013) (holding "[t]he fact that the impact of Defendant's conduct was felt [abroad] cannot deprive" plaintiffs of an ATS claim). The Ninth Circuit has observed that following *Kiobel*, courts have permitted ATS claims to go forward where "the plaintiffs have alleged that at least some of the conduct relevant to their claims occurred in the United States." *Mujica v. AirScan Inc.*, 771 F.3d 580, 595 (9th Cir. 2014) (collecting cases).

Moreover, in the context of a claim for aiding and abetting and conspiracy—like that alleged here—courts consistently consider all relevant domestic activity when assessing extraterritoriality and thus do "not limit[] their extraterritoriality inquiries to the situs of the direct tortious conduct." *Estate of Alvarez v. Johns Hopkins Univ.*, No. TDC-15-0950, 2022 U.S. Dist. LEXIS 71336, *36-37 (D. Md. Apr. 18, 2022).

Neither *Kiobel* nor *Nestlé* requires that all alleged conduct occur in the United States; they each simply found general allegations of corporate presence or general corporate activity insufficient. In *Kiobel*, the only alleged connection to the United States was the defendants' corporate presence. Similarly, in *Nestlé*, the plaintiffs alleged only that the defendant corporations had made unspecified "operational decisions" in the United States. The Supreme Court found that these "generic allegations," untethered to the claims alleged in the complaint, did "not draw a sufficient connection between the cause of action respondents seek – aiding and abetting forced labor overseas – and domestic conduct." 141 S. Ct. at 1937; *see also id.* ("As we

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

made clear in *Kiobel*, a plaintiff does not plead facts sufficient to support domestic application of the ATS simply by alleging 'mere corporate presence' of a defendant. . . . Pleading general corporate activity is no better.") (citing *Kiobel*, 569 U.S. at 125).[9]

Here, in contrast, the Complaint alleges far more than mere "general corporate activity" in the United States. The Individual Defendants developed the UAE's cyber-surveillance program while working for a U.S.-based company, operated under U.S. export control licenses that they violated, and recruited others from the United States. The Individual Defendants also purchased the Karma exploit and anonymization services from U.S. companies to create a hacking system specifically targeting Apple's U.S. servers, used computer hardware located and built in the U.S. in order to transmit malware into U.S. territory through U.S.-based servers, and utilized U.S.-based proxy servers to conceal their illegal activities. For such acts, the Individual Defendants were investigated and prosecuted by the U.S. Department of Justice. All of the Individual Defendants' acts, individually and collectively, amount to U.S.-based conduct that is directly relevant to Ms. Alhathloul's claim under the ATS for aiding and abetting and conspiracy to commit the crime against humanity of persecution.

B. The Complaint States a Claim for Persecution as a Crime Against Humanity.

Defendants' argument that the Complaint does not state a claim for persecution as a crime against humanity fails just as badly.

[9] Likewise, in *Hmong v. Lao People's Democratic Republic*, 748 F. App'x 136, 137 (9th Cir. 2019), the court emphasized that the plaintiff "did not allege *any* domestic conduct." (emphasis added), *aff'g* No. 2:15-cv-2349 TLN AC, 2016 U.S. Dist. LEXIS 76709 (E.D. Cal. June 13, 2016), *adopting* 2016 U.S. Dist. LEXIS 32746 (E.D. Cal. May 17, 2016) (noting "the *absence* of any possible connection to" the United States). Similarly, in *Balintulo v. Daimler AG*, the plaintiffs "failed to allege that *any* relevant conduct occurred in the United States," and "*[n]one* of [the allegations] . . . tie[d] the relevant human rights violations to actions taken within the United States." 727 F.3d 174, 189, 192 (2d Cir. 2013) (emphasis added).

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

First, U.S. courts have consistently held that crimes against humanity constitute a violation of the law of nations actionable under the ATS. *Kiobel v. Royal Dutch Petrol. Co.*, 621 F.3d 111, 116–20 (2d Cir. 2010) (recognizing that the ATS provides jurisdiction over crimes against humanity in accord with customary international law), *aff'd*, 569 U.S. 108 (2013); *Sosa v. Alvarez-Machain*, 542 U.S. 692, 760–62 (2004) (Breyer, J., concurring) (recognizing crimes against humanity as "universally condemned behavior" under international law that is cognizable under the ATS); *Mujica v. Occidental Petrol. Corp.*, 381 F. Supp.2d 1164, 1179-81 (C.D. Cal. 2005) (holding "there is a customary international law norm against crimes against humanity" sufficient for creating a cause of action under the ATS), *remanded on other grounds*, 564 F.3d 1190 (9th Cir. 2009); *Doe v. Rafael Saravia*, 348 F. Supp. 2d 1112, 1144, 1154–57 (E.D. Cal. 2004) (holding that "crimes against humanity meet the specific, universal, and obligatory standard" set forth in *Sosa* for ATS claims); *Mamani v. Berzain*, 654 F.3d 1148, 1152 (11th Cir. 2011) ("[T]his Court has decided that 'crimes against humanity' . . . may give rise to a cause of action under the ATS.").

Second, persecution constitutes a crime against humanity that is universally recognized as actionable under the ATS.[10] *See, e.g.*, *Doe v. Rafael Saravia*, 348 F. Supp. 2d 1112, 1144, 1154–57 (E.D. Cal. 2004) (holding that "persecution on political, racial or religious grounds" constitutes a crime against humanity actionable under the ATS); *Jane W.*, 560 F. Supp. 3d at 886 ("Persecution . . . the crime[] against humanity Plaintiffs seek liability under, [is]

[10] The elements of persecution are (i) the "denial of fundamental rights" contrary to international law; and (ii) "the intentional targeting of an identifiable group." *Lively*, 960 F. Supp. 2d at 317; *see also* ICC Elements of Crimes, Arts. 7(1)(h), 7(2)(g). The motion to dismiss does not contest that the Complaint adequately pleads both elements. An act of persecution rises to the level of a crime against humanity when committed in the context of "a 'widespread or systematic' attack against a civilian population." *Doe v. Qi*, 349 F. Supp. 2d 1258, 1308 (N.D. Cal. 2004).

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

actionable under the ATS."); *Sexual Minorities Uganda*, 960 F. Supp. 2d at 316–17 ("[P]ersecution that rises to the level of a crime against humanity has repeatedly been held to be actionable under the ATS."); *Wiwa v. Royal Dutch Petrol. Co.*, 626 F. Supp. 2d 377, 384–85 (S.D.N.Y. 2009) (political persecution constitutes a crime against humanity within the court's subject matter jurisdiction under the ATS); *Mehinovic v. Vuckovic*, 198 F. Supp. 2d 1322, 1352 & n.44 (N.D. Ga. 2002) ("persecutions on political, racial, or religious grounds," are "actionable under the ATCA"), *abrogated on other grounds by Aldana v. Del Monte Fresh Produce, N.A.*, 416 F.3d 1242, 1247 (11th Cir. 2005).

Indeed, persecution, which was prosecuted by the Nuremberg Tribunal following the Second World War, numbers among the very first crimes against humanity. *See, e.g.*, *Kiobel v. Royal Dutch Petrol. Co.*, 621 F.3d 111, 118–19 (2d Cir. 2010) (describing Nuremberg's pioneering prosecution of international human rights crimes, including persecution), *aff'd*, 569 U.S. 108 (2013); *Doe v. Rafael Saravia*, 348 F. Supp. 2d 1112, 1144, 1154–55 (E.D. Cal. 2004) (discussing the Nuremberg prosecutions, which effected the first recognition of the prohibition of crimes against humanity, including persecution, under international law). Defendants' bald contention that permitting a claim for persecution under the ATS would be an "unprecedented expansion of liability," Mot. to Dismiss at 9, and reference to it as "an *alleged* crime against humanity," *Id*. at 29 (emphasis added), must be rejected.

Third, the Complaint goes far beyond alleging the use of "technology to spy on" Ms. Alhathloul, as Defendants mischaracterize the claim. Mot. to Dismiss at 32. *See also id*. (incorrectly construing Plaintiff's claim as merely alleging "surveillance of foreigners"). The Complaint details how "the UAE has engaged in a widespread or systematic attack directed against a civilian population, namely perceived dissidents of the UAE and Saudi Arabia,

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

including human rights activists, journalists, academics, and other individuals viewed as expressing opinions critical of their respective autocratic regimes." The Complaint also shows that this included not only "hacking the devices and tracking the locations of members of the persecuted group," but also, *inter alia*, "imposing travel bans, and subjecting them to arbitrary arrests and detention, sham trials, torture, enforced disappearances, extrajudicial killings, as well as harassment and abuse of their family members." Compl. ¶ 172. The Defendants' hacking of Ms. Alhathloul's iPhone, and her subsequent detention and torture, is part of a larger, widespread and systematic campaign to target perceived dissidents with arbitrary detention, torture and forced disappearance. Compl. ¶¶ 32-49.

Fourth, the Complaint sets forth the widespread nature of the persecution of perceived dissidents, more than adequately alleging a crime against humanity. The Complaint notes that the U.S. Department of State Country Reports on the UAE and Saudi Arabia document the widespread nature of the persecution of individuals who criticize the governments of these two countries. Compl. ¶¶ 34-35, 44. For example, in a single incident, the UAE subjected 94 government critics and reform activists to a mass trial. *Id*. at paras. 36-37. Further, as part of this widespread attack, the Complaint alleges that Defendants repeatedly targeted perceived dissidents for hacking, including *hundreds* of iPhones. Compl. ¶ 60, 74, 82. This is more than sufficient to state a claim for a crime against humanity. *Doe v. Qi*, 349 F. Supp. 2d 1258, 1308 (N.D. Cal. 2004) ("The concept 'widespread' may be defined as massive, frequent, large scale action, carried out collectively with considerable seriousness and directed against a multiplicity of victims." (internal citations omitted)); *Prosecutor v. Blaškič*, No. IT-95-14-T, ¶ 206 (Trial Chamber, ICTY, March 3, 2000) (to determine whether an attack is sufficiently "widespread,"

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

courts can qualitatively and holistically consider "the cumulative effect of a series of inhumane acts or the singular effect of an inhumane act of extraordinary magnitude").[11]

Lastly, the Complaint sufficiently pleads the alternative criterion for a crime against humanity, namely that the attack be "systematic," referring to the "organized nature of the acts of violence and the improbability of their random occurrence." *Presbyterian Church of Sudan v. Talisman Energy, Inc.*, 226 F.R.D. 456, 481 (S.D.N.Y. 2005). The Complaint describes in detail the specific and coordinated targeting of individuals perceived by the UAE to be dissidents — including Alhathloul— and thus plainly alleges that her mistreatment was "systematic" in the sense that it was not accidental or random, but part of an organized pattern of abuse orchestrated against perceived dissidents, such as herself. Compl. ¶¶ 31–41. Further, as part of this systematic attack, the Complaint alleges that Defendants engineered sophisticated exploits and followed a regimented protocol to target perceived dissidents for hacking. Compl. ¶¶ 60–66, 78–86.

IV. DEFENDANTS ARE NOT ENTITLED TO ANY "FOREIGN OFFICIAL" IMMUNITY.

As a last gasp, Defendants argue they are somehow entitled to some form of foreign official immunity on the spurious ground that they are the UAE's "agents." Mot. to Dismiss at 33. The argument is without merit.

Defendants concede, as they must, that binding Circuit precedent forecloses any claim of common-law immunity for private corporate defendant DarkMatter. Mot. to Dismiss at 27 n. 5

[11] Defendants' argument that Alhathloul's allegations are insufficiently "widespread" because they purportedly "concern only herself and three other individuals" mischaracterizes the Complaint and, in any case, is unavailing. The single case that Defendants cite, *Mamani v. Berzaín*, 654 F.3d 1148, 1156 (11th Cir. 2011), does not suggest otherwise. Rather, it makes clear that there is no minimum number of victims required to support a finding of a crime against humanity.

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

("DarkMatter acknowledges that this argument is currently unavailable to DarkMatter under *WhatsApp Inc. v. NSO Group Technologies Limited*, 17 F.4th 930, 933 (9th Cir. 2021), which concluded that the Foreign Sovereign Immunities Act ["FSIA"], rather than common-law immunity, governs the sovereign immunity of non-natural persons."). Nor can DarkMatter avail itself of immunity under the FSIA because it is plainly not an "agency or instrumentality of a foreign state," which is defined in the statute as "any entity [that] is a separate legal person, corporate or otherwise, and . . . which is an organ of a foreign state or political subdivision thereof, or a majority of whose shares or other ownership interest is owned by a foreign state or political subdivision thereof." 28 U.S.C. § 1603(b)(1)-(2); *see also WhatsApp Inc.*, 17 F.4th at 940 (9th Cir. 2021) ("Whatever a private corporation's "government customers do with its technology and services does not render [it] an 'agency or instrumentality of a foreign state,' as Congress has defined that term."), *petition for cert. filed*, No. 21-1338 (U.S. Apr. 6, 2022).

Similarly, none of the Individual Defendants who worked for DarkMatter – a private corporation that is not an agency or instrumentality of a foreign state – is entitled to conduct-based foreign-official immunity, as a purported agent of the UAE or otherwise. Such immunity does not extend to private contractors. *See Doğan v. Barak*, 932 F.3d 888, 893-894 (9th Cir. 2019) (citing Restatement (Second) of Foreign Relations Law § 66(f) (1965)) ("Common-law foreign sovereign immunity extends to individual *foreign officials* for 'acts performed in [their] *official capacity*'") (emphasis added).

Further, even assuming *arguendo* that the Individual Defendants were eligible to claim conduct-based foreign-official immunity, which they are not, whether such an immunity actually applies is determined via a "two-step procedure"—nowhere mentioned by the Defendants—that considers: (1) whether "the diplomatic representative of the sovereign [] request[s] a 'suggestion

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

of immunity' from the State Department"; and (2) absent a suggestion of immunity ("SOI"), "whether the ground of immunity is one which it is the established policy of the State Department to recognize." *Samantar v. Yousuf*, 560 U.S. 305, 311-12 (2010). Here, the Individual Defendants fail both steps. First, the State Department has not filed an SOI. Nor have the Individual Defendants presented proof that the diplomatic representative of the UAE has even requested one. Second, the Individual Defendants' putative "ground of immunity" does not fall within any established policy recognized by the State Department, and none is cited by Defendants. Defendants' conduct-based foreign-official immunity claim thus fails on multiple grounds.

CONCLUSION

For the foregoing reasons, Defendants' Motion to Dismiss should be denied.

Certificate of Compliance

This brief complies with the applicable word-count limitation under L.R. 7-2(b), with leave granted by the Court to exceed the page limitation by no more than ten pages or 2,000 words, (*see* DE 34) because it contains 12,985 words, including headings, footnotes, and quotations, but excluding the caption, table of contents, table of cases and authorities, signature block, exhibits, and any certificates of counsel.

Dated: July 21, 2022

Respectfully submitted,

BOISE MATTHEWS LLP

/s Bridget Donegan
Bridget M. Donegan
OSB No. 103753

BOISE MATTHEWS LLP
805 SW Broadway, Suite 1900
Portland, OR 97205
Telephone: (503) 228-0487
Facsimile: (503) 227-5984

805 SW Broadway, Suite 1900
Portland, OR 97205
(503) 228-0487
bridget@boisematthews.com

FOLEY HOAG LLP
Christopher E. Hart
MA BBO No. 625031
Anthony D. Mirenda
MA BBO No. 550587
Andrew Loewenstein (*pro hac vice pending)*
MA BBO No. 648074
155 Seaport Boulevard
Boston, MA 02210
(617) 832-1000
chart@foleyhoag.com
adm@foleyhoag.com
aloewenstein@foleyhoag.com

ELECTRONIC FRONTIER FOUNDATION
Sophia Cope (*pro hac vice pending)*
CA Bar No. 233428
David Greene
CA Bar No. 160107
Mukund Rathi
CA Bar No. 330622
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
sophia@eff.org
davidg@eff.org
mukund@eff.org

Attorneys for Plaintiff Loujain Hathloul Alhathloul